

CHAPTER 3:ALGEBRAIC STRUCTURE PART 2

Dr. Djohra MEGUEDMI

Algebra 1.

November 2023



OUTLINES OF THIS TALK

- ① Ring and Sub-ring
- ② Ring homomorphisms
- ③ Fields
- ④ Exercises

DEFINITION

- ① A ring is a set together with two binary operations called addition and multiplication satisfying the following axioms:

- ① $(R, +)$ is an Abelian group.
- ② \times is associative
- ③ The following distributive laws hold:

$$(a + b)c = ac + bc \quad \text{and} \quad a(b + c) = ab + ac.$$

- ② The ring R is commutative if multiplication is commutative.
③ The ring R is said to have an identity if there is an element $1_R \in R$ such that

$$1_R \times a = a = a \times 1_R \quad \forall a \in R.$$

Then $(R, +, \times)$ is called a **ring**.

EXAMPLE

- ① $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$ are commutative rings with usual operations of addition and multiplication.
- ② The set of non-negative integers \mathbb{Z}^+ is not a ring as $(\mathbb{Z}^+, +)$ is not an abelian group.
- ③ The set of even integers $2\mathbb{Z}$ is a commutative ring, but it is not an identity one.

PROPOSITION

Let R be a ring. Then,

- ① $0_R a = a0_R = 0_R, \quad \forall a \in R.$
- ② $(-a)b = a(-b) = -(ab), \quad \forall a, b \in R.$
- ③ $(-a)(-b) = ab, \quad \forall a, b \in R.$
- ④ if R has an identity then the identity is unique and
 $-a = (-1_R)a, \quad \forall a \in R.$

DEFINITION

Let R be a ring.

- ① An element $a \neq 0_R \in R$ is called a zero divisor if there is $b \neq 0_R \in R$ such that $ab = 0_R$ or $ba = 0_R$.
- ② Suppose that R has an identity $1_R \neq 0_R$. An element $u \in R$ is called a unit in R if there is some $v \in R$ such that $uv = vu = 1_R$.

NOTE

- ① The set of units of R is denoted $U(R)$.
- ② $U(R)$ is a group under multiplication referred to as the group of units.
- ③ A zero divisor can never be a unit.

EXAMPLE

$$\begin{aligned}U(\mathbb{Z}) &= \{+1, -1\} . \\U(\mathbb{Z}/8\mathbb{Z}) &= \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}.\end{aligned}$$

DEFINITION

An integral domain is a commutative ring without zero-divisor.

In other words, a commutative ring \mathbf{R} is an integral domain if, and only if,

$$\forall a, b \in \mathbf{R}, ab = 0 \Rightarrow a = 0 \vee b = 0.$$

EXAMPLE

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and \mathbb{C} are integral domains.

The ring $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain since we have :

$$\bar{2} \otimes \bar{3} = \bar{6} = \bar{0}.$$

THEOREM

Let \mathbf{R} be a ring. If a and b are elements in \mathbf{R} which commute $ab = ba$, then we have for all $n \in \mathbb{N}$

$$(a + b)^n = \sum_{k=0}^{k=n} \binom{n}{k} \cdot a^k b^{n-k}$$

DEFINITION

Let $(R, +, \times)$ a ring. A subset S of R is a subring of $(R, +, \times)$ if we have :

- ① $(S, +)$ is a subgroup of $(R, +)$
- ② S is closed under multiplication: $\forall a, b \in S, ab \in S$.
- ③ $1_R \in S$

EXAMPLE

- ① \mathbb{Z} is the only subring of \mathbb{Z}
- ② \mathbb{Z} is a subring of \mathbb{Q} , which is a subring of \mathbb{R} , which is a subring of \mathbb{C}
- ③ $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\}$ is a subring of \mathbb{C} .

PROPOSITION

Characterization of sub-rings Let $(R, +, \times)$ a ring and $S \subset R$, S is a subring of $(R, +, \times)$ iff:

- ① $1_R \in S$
- ② $\forall a, b \in S, a - b \in S$
- ③ $\forall a, b \in S, a \times b \in S$

DEFINITION

Let R and R' be rings.

- ① A ring homomorphism is a map $\phi : R \rightarrow R'$ satisfying
 - ① $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$.
 - ② $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.
- ② The kernel $\ker(\phi)$ of ϕ is defined as
$$\ker(\phi) = \{r \in R : \phi(r) = 0'_R\}.$$
- ③ A bijective ring homomorphism is called a ring isomorphism.

DEFINITION

Let R and R' be rings.

- ① A ring homomorphism is a map $\phi : R \rightarrow R'$ satisfying
 - ① $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$.
 - ② $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$.
- ② The kernel $\ker(\phi)$ of ϕ is defined as
 $\ker(\phi) = \{r \in R : \phi(r) = 0'_R\}$.
- ③ A bijective ring homomorphism is called a ring isomorphism.

PROPOSITION

Let R and R' be rings and let $\phi : R \rightarrow R'$ be a homomorphism.

- ① The image of ϕ is a subring of R' .
- ② $\ker(\phi)$ is a subring of R with the additional property that for all $r \in \ker(\phi)$ and $a \in R$, $ra, ar \in \ker(\phi)$.

THEOREM

Let $\phi : R \longrightarrow R'$ be a ring homomorphism. Then we have

- ① $\phi(0) = 0'$
- ② $\phi(na) = n\phi(a), \forall a \in R, \forall n \in \mathbb{Z}$.
- ③ $\phi(a^n) = (\phi(a))^n, \forall a \in R, \forall n \in \mathbb{Z}$.
- ④ $\phi(a^n) = (\phi(a))^n, \forall a \in U(R), \forall n \in \mathbb{Z}$.
- ⑤ $\phi^{-1}(B)$ is a subring of R , for all subring B of R' .

REMARK

Isomorphisms, endomorphisms and automorphisms are defined similarly to those of groups.

DEFINITION

Let R be a ring, let $I \subseteq R$ and let $r \in R$.

- ① $rl = \{ra : a \in I\}$ and $Ir = \{ar : a \in I\}$.
- ② A subset I of R is a left ideal or R if
 - ① I is a subring of R , and
 - ② $rl \subseteq I$ for all $r \in R$.
- ③ A subset I of R is a right ideal or R if
 - ① I is a subring of R , and
 - ② $Ir \subseteq I$ for all $r \in R$.
- ④ A subset I that is both a left ideal and right ideal is called an ideal.
- ⑤ if R is commutative we have $rl = Ir$

EXAMPLE

$\forall n \in \mathbb{Z}$, $n\mathbb{Z}$ is an ideal of \mathbb{Z} .

DEFINITION

Let R be a commutative ring, and let I be an ideal of R . The relation \mathcal{R} defined on R by

$$\forall x, y \in R, x\mathcal{R}y \Leftrightarrow x - y \in I,$$

is an equivalence relation. The quotient set will be denoted by R/I . We define on A/I the two binary operations:

$$\forall \bar{x}, \bar{y} \in A/I, \bar{x} + \bar{y} = \overline{x + y} \text{ and } \bar{x} \cdot \bar{y} = \overline{xy}.$$

THEOREM

R/I is a commutative ring under the operations defined above. It is called the quotient ring.

DEFINITION

A field is a commutative ring in which every nonzero element is invertible.

DEFINITION

A subfield of a field is a subring which is itself a field.

EXAMPLE

\mathbb{Q} , \mathbb{R} and \mathbb{C} , endowed with usual operations, are fields. \mathbb{Z} is not a field.

THEOREM

The ring $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if, p is prime.